Pathlock Support for the Department of Defense Zero Trust Reference Architecture

Implementing a Secure, Data-Centric, Zero Trust Architecture

AT A GLANCE

Reduce Access Risks in the Face of an Increasingly Complex Threat Landscape

The Department of Defense Zero Trust Reference Architecture (DoD ZT-RA) serves as a critical framework for the DoD in its mission to safeguard sensitive data, operations, and assets against a variety of cyber threats. Traditional security models often operate on the assumption that anything inside the network is trustworthy. However, with the increasing sophistication of threats – internal and external - this assumption can no longer be allowed. Taking a Zero Trust stance ensures that access is strictly authenticated and continuously monitored, regardless of where it originates.

This brief describes how Pathlock, the leader in application access governance and cybersecurity controls automation, allows DoD stakeholders to implement Zero Trust in alignment with the DoD ZTA-RA via a proven, scalable solution.

SUPPORT FOR THE GOALS OF THE ZERO TRUST REFERENCE ARCHITECTURE

The DoD has set out five (5) goals for the DoD ZT-RA that Pathlock actively supports to enable effective security and defense of DoD information, systems, and infrastructure.

Modernize Information Enterprise to Address Gaps and Seams

Pathlock provides a risk-centric view of user activities across business applications and processes. This centralized visibility is essential for a Zero Trust model, where it is paramount to understand who has access to what and what they're doing with that access.

Simplify Security Architecture

As an integrated, cross-application solution, Pathlock removes the need for multiple disparate access control solutions for various applications and platforms. Pathlock offers a centralized solution that reduces the complexity of managing multiple systems, thereby simplifying the overall security architecture.

Produce Consistent Policy

A core capability of Pathlock is its centralized policy management dashboard. This allows administrators to define, review, and modify access policies from a single location, ensuring that policies are consistently applied across all integrated systems.

Optimize Data Management Operations

Pathlock can uniquely consolidate access data across the myriad systems within the DoD, providing a holistic view of who has access to what, making data management more streamlined and effective. Also, Pathlock's continuous monitoring and periodic user access reviews can identify and eliminate redundant or unnecessary access permissions. This cleanup not only enhances security but also simplifies data management operations by reducing unnecessary complexity.

Provide Dynamic Credentialing and Authorization

Pathlock continuously evaluates access requests against the set policies in real-time, ensuring that decisions are made based on the most recent data and context. This dynamic evaluation ensures that users only get access when and where appropriate. Furthermore, access decisions can be made based on contextual factors such as user location, device type, current role, recent activities, and more. This means that a user might be granted access under one set of circumstances but denied under another, adding a dynamic layer to the access control.

Pathlock Support for the Department of Defense Zero Trust Reference Architecture

Implementing a Secure, Data-Centric, Zero Trust Architecture

ZERO TRUST PILLARS

The DoD Zero Trust Reference Architecture defines seven Zero Trust Pillars, each mapping to various underlying requirements. The Pathlock suite of products addresses many of these capabilities, as shown in the following grid.

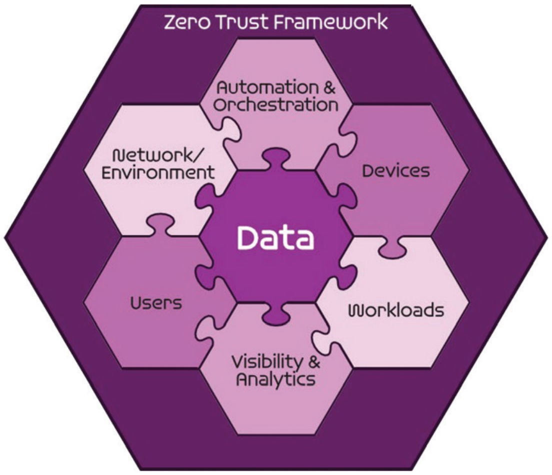

Figure 1: Zero Trust Pillars

Zero Trust (ZT) Pillars were identified by the ZT Strategy. These associate to an interlinked group of strategic resources.

Protecting data is at the center of ZT goals and is a part of all other resources.

All the resources are bound into the Zero Trust Framework.

(This image appears on page 22 of *Department of Defense Zero Trust Architecture Version 2.0.*)

PATHLOCK SUPPORT FOR THE DoD ZT-RA

ZERO TRUST	CORE PILLARS						
	User	Device	Applications and Workloads	Data	Network and Environment	Automation and Orchestration	Visibility and Analytics
CORE CAPABILITIES	🟩 User Inventory	⬜ Device Inventory	▨ Application Inventory	🟩 Data Catalog Risk Alignment	⬜ Data Flow Mapping	🟩 Policy Decision Point & Policy Orchestration	🟩 Log All Traffic (Network, Data, Apps, Users)
	🟩 Conditional User Access	⬜ Device Detection and Compliance	🟩 Secure Software Development & Integration	🟩 DoD Enterprise Data Governance	⬜ Software Defined Networking	🟩 Critical Process Automation	🟩 Security Information and Event Management
	⬜ Multi-Factor Authentication	⬜ Device Auth w/ real-time inspection	🟩 Software Risk Management	🟩 Data Labelling and Tagging	⬜ Macro Segmentation	🟩 Machine Learning	🟩 Common Security and Risk Analytics
	🟩 Privileged Access Management	⬜ Remote Access	▨ Resource Authorization & Integration	⬜ Data Monitoring and Sensing	🟩 Micro Segmentation	⬜ Artificial Intelligence	🟩 User and Entity Behavior Analytics
	🟩 Identity Federation & User Credentialing	▨ Partially & Fully Automated Asset, Vuln. and Patch Management	🟩 Continuous Monitoring and Ongoing Authorizations	⬜ Data Encryption & Rights Management		🟩 Security Orchestration Automation & Response	🟩 Threat Intelligence Integration
	▨ Behavioral, Contextual ID and Biometrics	⬜ Unified End Point Mgmt. & Mobile Device Mgmt.		🟩 Data Loss Prevention		🟩 API Standardization	🟩 Automated Dynamic Policies
	🟩 Least Privileged Access	⬜ Endpoint & Extended Detection & Response		🟩 Data Access Control		🟩 Security Operations Center & Incident Response	
	🟩 Continuous Authentication						
	🟩 Integrated ICAM Platform						

LEGEND

🟩 Supported by Pathlock ▨ Partially Supported by Pathlock ⬜ Not Supported by Pathlock

pathlock

SOLUTION OVERVIEW

Pathlock Support for the Department of Defense Zero Trust Reference Architecture

Implementing a Secure, Data-Centric, Zero Trust Architecture

IMPLEMENTING THE DEPARTMENT OF DEFENSE (DOD) ZERO TRUST REFERENCE ARCHITECTURE USING PATHLOCK

User:

1.1 User Inventory: The Pathlock product suite maintains an inventory of users and monitored applications and uses access rules to control access to the applications and systems.

1.2 Conditional User Access: The Pathlock product suite uses policies that consider users, data, and context of access to provide conditional access to users to access data in the enterprise systems.

1.3 Privileged Access Management: Pathlock Privileged Access Management focuses on removing administrator/elevated privileges by using time-limited access, automating privilege access approvals, and logging all elevated access on the monitored systems.

1.4 Identity Federation & User Credentialing: The Pathlock product suite uses a centralized identity repository to store users and to standardize identity lifecycle management.

1.5 Behavioral, Contextual ID, and Biometrics: The Pathlock product suite uses user and contextual attributes that can be combined with organizational-specific attributes to enhance access control.

1.6 Least Privileged Access: The Pathlock product suite focuses on provisioning the minimum access required to perform tasks and helps periodically review the accessing and fine-tuning access in terms of the roles assigned to the user.

1.7 Continuous Authentication: The Pathlock product suite uses attribute-based authentication that continuously checks users and groups accessing data in the monitored systems.

Device:

2.1 Partially & Fully Automated Asset, Vulnerability, and Patch Management: The Pathlock Cybersecurity product suite helps automate patch management for monitored ERP systems and supports hybrid patch management.

Applications and Workload:

3.1 Application Inventory: The Pathlock product suite keeps a record of all the applications that use the Pathlock connector network to connect to SAP ERP systems. Only the authorized applications, as approved by the appropriate authorizing official, are allowed to connect to the SAP systems through the Pathlock connector network.

3.2 Secure Software Development & Integration: The Pathlock product suite follows software and application security processes throughout the product development lifecycle, including best practices and controls such as code review, transport controls, and code scanning.

3.3 Software Risk Management: The Pathlock product development lifecycle follows procedures to secure all product components by implementing controls for the coding and transporting of objects and packaging.

3.4 Resource Authorization & Integration: The Pathlock product suite reviews user and data security posture and utilizes an authorization policy and a checks-based approach to limit access to resources, enabling the removal of access when not needed.

3.5 Continuous Monitoring and Ongoing Authorizations: The Pathlock product suite uses a dynamic attribute-based policy approach to continuously check application data access based on the users and the data being accessed, thereby ensuring the security of monitored applications.

Pathlock Support for the Department of Defense Zero Trust Reference Architecture

Implementing a Secure, Data-Centric, Zero Trust Architecture

Data:

4.1 Data Catalog Risk Alignment: The Pathlock product suite helps data owners identify and catalog sensitive data in the landscape, and any changes to the data affecting its sensitivity are detected and adjusted in the catalog accordingly.

4.2 DoD Enterprise Data Governance: Pathlock uses access control policies and data tagging at the field level to ensure appropriate user action on enterprise data.

4.3 Data Labeling and Tagging: The Pathlock product suite helps identify and tag sensitive data to ensure that the right user has access to the right data at the right time.

4.4 Data Loss Prevention: The Pathlock product suite uses threat detection to identify potential threats and uses dynamic access control policies to prevent data exfiltration from the SAP systems.

4.5 Data Access Control: The Pathlock product suite uses data and user attributes to ensure appropriate access to and use of data, ensuring that any unauthorized user cannot access data.

Network and Environment:

5.1 Micro-Segmentation: The Pathlock product suite uses programmatic approaches to apply policies to enable network segmentation using user identity and data for application access.

Automation and Orchestration:

6.1 Policy Decision Point & Policy Orchestration: The Pathlock Policy Controller is native to the monitored enterprise system and can enforce all rule-based policies to orchestrate access across the monitored systems to ensure appropriate user access.

6.2 Critical Process Automation: Several critical processes can be automated using dynamic access controls that use the properties of the users, data, and the context of data access to automate data access and usage.

6.3 Machine Learning: The Pathlock product suite uses dynamic rules to execute critical functions such as mitigation response, anomaly detection, and user blocking.

6.4 Security Orchestration Automation & Response: The Pathlock product suite uses pre-defined rulesets from pre-packaged content to improve security operations, threat, and vulnerability management through real-time visibility that helps accelerate a security team's response time.

6.5 API Standardization: The Pathlock connector framework provides an enterprise-wide API standard to improve application interfaces and enhance interoperability.

6.6 Security Operations Center (SOC) & Incident Response (IR): The Pathlock Cybersecurity product suite provides security monitoring, protection, and responses by providing real-time visibility and mitigation responses.

Visibility and Analytics:

7.1 Log All Traffic (Network, Data, Apps, Users): The Pathlock product suite logs all monitored activities and makes those logs available for security administrators to generate data usage reports by specific users or applications.

7.2 Security Information and Event Management (SIEM): The Pathlock cybersecurity dashboard monitors, detects, and analyzes data logged and triggers alerts and mitigation actions to common threat events.

7.3 Common Security and Risk Analytics: The Pathlock platform supports the detection of anomalous users, actions, and threat detection based on rules and policies on data collected from the different monitored systems.

7.4 User and Entity Behavior Analytics: The Pathlock executive dashboard provides a centralized view of users and application data access to support the detection of anomalous users and advanced threat detection.

7.5 Threat Intelligence Integration: Pathlock's integrated threat intelligence and data collected from all the monitored application logs enhance monitoring and incident response.

7.6 Automated Dynamic Policies: Pathlock's dynamic policies for access control, threat detection, and vulnerability management continuously monitor risk and automate the triggering of alerts and mitigation actions for evolving risks, threats, and patch management.

LEVERAGING PATHLOCK TO OPERATIONALIZE THE DoD ZT-RA

Pathlock is a pivotal tool in the quest to operationalize the Department of Defense's Zero Trust Reference Architecture (DoD ZT-RA). As the recognized market leader in application access governance, its capabilities align seamlessly with the fundamental principles of the Zero Trust model.

Through its centralized policy management, Pathlock ensures consistent and unified access governance across diverse systems, laying the groundwork for a more secure and streamlined environment. Its dynamic, context-aware authorization mechanisms address the need for real-time, adaptive security ensuring that users have the right access under the right conditions.

The platform's continuous monitoring, integration capabilities with external identity providers, and support for attribute-based access control further amplify its value, allowing the DoD to maintain a robust security posture while optimizing data management operations. In essence, employing Pathlock provides the DoD with an efficient, effective, and adaptive means to navigate the complexities of the modern digital landscape, ensuring compliance with the tenets of the ZT-RA.

REFERENCE MATERIAL

1. Department of Defense Zero Trust Architecture Version 2.0 (https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)

About Pathlock

The Pathlock platform protects the leading ERP systems, enterprise business applications and the critical transactions they power. Our application governance solutions help companies enforce GRC controls and take action to prevent loss. Enterprises can manage all aspects of application governance in a single platform, including user provisioning and temporary elevation, ongoing user access reviews, control testing, transaction monitoring, and audit preparation.

8111 Lyndon B Johnson Fwy,
Dallas, TX 75251
Phone: +1 469.906.2100
info@pathlock.com